2

Secure Processing From the Desktop: A Policy for Using Personal Workstations to Process Restricted Company Information

MP 94B0000016
February 1994

Leonard J. LaPadula
James G. Williams

MITRE
Bedford, Massachusetts

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY (Leave blank)

2. REPORT DATE
February 1994

3. REPORT TYPE AND DATES COVERED

4. TITLE AND SUBTITLE
Secure Processing From the Desktop: A Policy for Using Personal Workstations to Process Restricted Company Information

5. FUNDING NUMBERS

6. AUTHOR(S)
Leonard J. LaPadula, James G. Williams

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
The MITRE Corporation
202 Burlington Road
Bedford, MA 01730-1420

8. PERFORMING ORGANIZATION REPORT NUMBER
MP 94B0000016

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT (Maximum 200 words)

Corporate data communications networks are rapidly becoming major information exchange resources for the companies they serve. They can easily provide the underlying services needed to share unclassified, non sensitive technical and administrative information throughout an enterprise. Increasingly, however, there may be a need to exchange sensitive or critical information of various kinds. Inevitably this will lead to requirements for safeguards to protect confidentiality, to preserve integrity, and to ensure availability. During 1993, the Information Security Technical Center of The MITRE Corporation developed a policy in anticipation of such needs. The first step was to define the information and functional requirements. For this purpose, restricted MITRE information was chosen as the focus. This category of sensitive information includes privileged memos, performance evaluations, business plans, and salary data; in general, it encompasses executive, financial, and personnel data. The second step was to develop a security policy governing the processing of restricted information on the desktop - on personal workstations with corporate inter computer networking capability. Such a policy defines responsibilities of employees as well as technical requirements for automated processing in the desktop environment. The third step, currently underway, is to evaluate commercial products that may meet the requirements of the policy. In developing the security policy, we kept in mind the goal of requiring the minimum additional software and hardware consistent with acceptable risk. The result is that we can implement the policy with low-cost, commercially available, add-on software. Thus, the policy may be of great interest to enterprises having a similar need to handle restricted information.

14. SUBJECT TERMS
corporate data, networks, security

15. NUMBER OF PAGES
27

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	Unlimited

Secure Processing From the Desktop: A Policy for Using Personal Workstations to Process Restricted Company Information

MP 94B0000016
February 1994

Leonard J. LaPadula
James G. Williams

Contract Sponsor N/A
Contract No. N/A
Project No. JOCEA
Dept. G020

Approved for public release;
distribution unlimited.

MITRE
Bedford, Massachusetts

ABSTRACT

Corporate data communications networks are rapidly becoming major information exchange resources for the companies they serve. They can easily provide the underlying services needed to share unclassified, nonsensitive technical and administrative information throughout an enterprise. Increasingly, however, there may be a need to exchange sensitive or critical information of various kinds. Inevitably this will lead to requirements for safeguards to protect confidentiality, to preserve integrity, and to ensure availability. During 1993, the Information Security Technical Center of The MITRE Corporation developed a policy in anticipation of such needs. The first step was to define the informational and functional requirements. For this purpose, restricted MITRE information was chosen as the focus. This category of sensitive information includes privileged memos, performance evaluations, business plans, and salary data; in general, it encompasses executive, financial, and personnel data. The second step was to develop a security policy governing the processing of restricted information on the desktop — on personal workstations with corporate intercomputer networking capability. Such a policy defines responsibilities of employees as well as technical requirements for automated processing in the desktop environment. The third step, currently underway, is to evaluate commercial products that may meet the requirements of the policy. In developing the security policy, we kept in mind the goal of requiring the minimum additional software and hardware consistent with acceptable risk. The result is that we can implement the policy with low-cost, commercially available, add-on software. Thus, the policy may be of great interest to enterprises having a similar need to handle restricted information.

TABLE OF CONTENTS

LIST OF TABLES

INTRODUCTION

This paper deals with policy specification, the second of three phases in supporting MITRE's Information Security Technical Center's effort titled *Secure Processing from the Desktop* (SPD). The other two phases deal with requirements identification and capabilities development.

PURPOSE OF SPD TASK

Increasing dependence on desktop processing of information in a networked environment makes special handling of restricted information by manual methods inefficient and inconvenient. In a networking environment where everyone's desktop computer is potentially a server, the opportunities for effective sharing of information keep growing but currently have outpaced our ability to protect various classes of restricted information. The SPD task's purpose is to demonstrate the feasibility of securely exchanging corporate restricted information on the MITRE corporate network. The approach is to provide capabilities for managers in the Information Systems Security division to use their desktop computing capabilities to store, process, and share certain restricted corporate information in a manner consistent with corporate security policy.

TASK APPROACH

The SPD task has three major parts.

- Processing Requirements Identification
- Policy Specification
- Capabilities Development

Identification of processing requirements entailed interviewing several G020 managers to develop a profile of the sensitive information they would like to process with their desktop computing capabilities. From this profile the SPD task defined the category of information to be protected and the security relevant processing requirements for that information. The single category of information includes types of information that require similar kinds and levels of protection and for which there is a common authority. The processing requirements include all the needed functions for a user to process the chosen category of information in the desktop computing environment.

Policy specification starts with a summary of existing, relevant MITRE policy on proper handling and automated processing of privileged, proprietary, and unclassified but sensitive information. From this basis, the task develops a security policy for desktop processing of the informational category and functional capabilities identified in the processing requirements definition. Development of the security policy includes threat analysis based on the computing environment for the desktop processing.

Capabilities development begins with a survey of products that appear relevant to the desired processing capabilities. By mapping the security requirements defined in the policy specification part of the task to services and mechanisms designed to counter threats and by then mapping these services and mechanisms to the surveyed products, a useful subset of the products is selected. From this subset the task will implement one or more capabilities for the Information Security Technical Center managers.

COMPUTING ENVIRONMENT

The MITRE corporate network supports a variety of intercomputer networking capabilities among a large set of different computers. There are, however, several major types relevant to desktop processing—Macintoshes, PCs, and the SUN family of workstations. Their operating systems characterize the computing environment: they are System 7, Windows 3.1, and various UNIX implementations. Each of these operating environments provides some form of client-server networking capability and it is possible to communicate among them. Besides consideration of these workstation types, this task must also consider the numerous servers that provide capabilities for the various client-server facilities.

The desktop systems attach to the MITRE corporate network in a variety of ways, some of them having more than one attachment. The corporate network uses a backbone Ethernet topology, incorporating routers, gateways, and bridges to connect multiple LANs into a local internet. The corporate network is divided into a trusted zone and an untrusted zone. Most of the corporate network is in the trusted zone. No constraints on intercomputer networking are imposed in the trusted zone. The untrusted zone provides limited internetworking service to MITRE personnel in physical areas that are not under MITRE control. The general service available to workstations in the untrusted zone is challenged login, via SecurId card, to one of several boundary hosts within the trusted zone, using TCP/IP for transport service. Boundary hosts are specially programmed to require the SecurId card login and to restrict access to certain TCP ports. In this way, boundary hosts provide network access control over users from the untrusted zone and from outside MITRE to services within the trusted zone.

All of the workstation types of interest for this task potentially can access the entire trusted zone of the MITRE corporate network, and, through the boundary hosts, they can gain access to computers, for which their users have accounts, located outside MITRE. In addition to TCP/IP-based services available to all workstations having the necessary software installed, the Macintoshes generally have AppleShare capabilities through AppleTalk data communications and the PCs have various intercomputer networking capabilities using Novell clusters for data communications.

The SPD task makes the assumption that intercomputer networking in support of processing restricted MITRE information takes place within the trusted zone of the MITRE corporate network. The threat environment would, of course, be radically harsher if this assumption were weakened to allow exchange of restricted MITRE information across the trust boundary. This assumption of the task translates into an explicit user requirement to remain inside the trusted zone when processing restricted MITRE information on the network.

Thus, the SPD task addresses requirements, policy, and capabilities for processing restricted information on Macintoshes, PCS, UNIX-based workstations, and various servers and for intercomputer sharing of restricted information within the trusted zone of the MITRE corporate network.

INFORMATIONAL AND FUNCTIONAL CONTEXT

We summarize the context here, from our complete analysis of the informational and functional context. The informational requirements are characterized by the single category of information called "restricted MITRE information". This category consists of MITRE executive, personnel, and financial data, such as business plans, performance reviews, and salary information.

> **Restricted MITRE Information**: Information about MITRE, including its plans, its finances, and its personnel, which for reasons of ordinary prudence, inherited responsibility, or privacy of the corporation or individuals should be restricted to viewing and handling by authorized individuals only. Restricted MITRE information includes executive, financial, and personnel information.

The SPD task constrains itself to dealing with restricted MITRE information as just defined. There are other classes of information for which policies similar to the proposed policy in this paper could be defined. Our expectation is that, upon demonstrating the successful implementation of the limited policy exhibited herein, the approach used and much of the policy defined will be extended to other classes of information dealt with in the MITRE environment.

The functional requirements are summarized in table 1.

Table 1. Summary of Functional Requirements for Restricted MITRE Information

Functional Capabilities	
Category	**Description**
Personal workstation, ordinary processing	Process restricted MITRE information on the personal workstation using the same applications as for nonrestricted information
Personal workstation, system administration	Administrator has access to personal workstation without access to restricted information
Personal workstation, operating environment	Preserve the look and feel of current systems
Personal workstation, storage	Store restricted information on personal workstations, even when the user is not present
Personal workstation, portable	Security controls for PowerBooks, especially object-reuse
Server, storage	Store restricted information on servers
Network, transmission	Share restricted information by electronic transmission on MITRE corporate network
Network, printing	Send restricted information to printer on network
Compound, file sharing	Share restricted information by remote access file sharing among personal workstations

We further focus the scope of the task with respect to the desktop environment for the selected information processing. Although all of the managers and administrative personnel likely to be affected by the SPD task's policy specification either have Macintosh computers or IBM PC clones, we also include UNIX-based workstations within the scope of policy specification. Besides being employed as desktop computers, many of these workstations also function as servers in various client-server arrangements. Recently, the PRISM organization published a policies and procedures manual for personal computers [1], in which it defined computer systems running DOS-based, Windows-based, or Macintosh operating systems with an Intel or Apple processor as personal computers. The SPD task has adopted the same terminology, as reflected in the glossary of this document. Thus, to reflect the scope of desktop environments for the SPD task we will use the term *personal workstation* to designate UNIX-based workstations as well as personal computers as defined by PRISM.

PRELIMINARIES TO PROPOSED SECURITY POLICY

This section summarizes relevant portions of existing MITRE policy governing automated processing of restricted information, describes the scope and structure of the new, proposed security policy, and explains any special notions needed for the proposed policy.

CURRENT SECURITY POLICY

Current MITRE policy for automated processing of sensitive information is defined in the MITRE Policies & Procedures [2] and the MITRE Security Procedures [3]. It focuses primarily on confidentiality in specifying general policy requirements. This policy does not give explicit requirements for automated handling of restricted information as defined for the SPD task. Nevertheless, a basis for policy can be inferred from these documents. Appendix 1 contains excerpts relevant to this effort. In this section those excerpts are interpreted to form a policy basis. The first two policy statements are general requirements and the third is a technical requirement.

Interpretation of MITRE P&P: Section B.2.e: Protection of Unclassified Computers and Data Communications Systems, Part G

General Requirements for MITRE Employees: Any MITRE employee who intentionally intercepts wire or electronic communications without authorization, intentionally obtains access to information in networks or computers without authorization, or intentionally exceeds access permissions without authorization is in violation of the Electronic Communications Privacy Act of 1986 (US law) and is subject to criminal fines and penalties, civil damages, and corporate disciplinary action which may include termination of employment.

Interpretation of MITRE P&P: Section F.1.c: Identification of Privileged Correspondence or Communications: Section III, Parts A, B, and C

Safeguards for Restricted MITRE Information: Restricted MITRE information, whether in hard copy or electronic form, shall have appropriately restricted distribution, shall be safeguarded from casual inspection when not in use, and shall be appropriately disposed of when no longer needed. Distribution is appropriately restricted when explicit controls are employed to ensure that only authorized, intended personnel receive the information. For hard copy of the information, restricted distribution is normally ensured by an attached distribution list. Casual inspection of not-in-use hard copy is normally prevented by placing the hard copy in a locked container. Disposal of the restricted information in hard copy form is appropriate when the likelihood of retrieval by unauthorized people is very small. For hard copy this is normally done by disposing of it in a classified waste receptacle or by using a shredder.

Interpretation of MITRE Security Procedures: Section 23: Unclassified Computers and Data Communications Systems: Paragraph 2311: Virus Protection

***Technical Requirement for Safeguarding Computer Software Used for Processing Restricted MITRE Information*:** Only software from known, reliable sources shall be installed and used on computers in the MITRE workplace. Software of unknown origin, including software acquired from public bulletin board systems, shall not be used. Sc^t-vare obtained from noncommercial sources shall be tested several times before installation. Anti-virus software shall be used on all personal workstations.

The last requirement, although it can counter the threat of disclosure of information by Trojan horses, also provides protection against loss of integrity and availability. Similarly, some of the requirements in the proposed security policy of the next section address integrity and availability issues as well as confidentiality. However, confidentiality remains the principal concern of the policy, not because integrity and availability are less important but because the task has limited resources in fiscal year 1993.

All of these requirements from current policy are reflected in the proposed security policy. However, the elements of these requirements have been reorganized and interpreted to fit the needs of the proposed policy.

SCOPE AND STRUCTURE OF THE PROPOSED POLICY

This proposed policy governs the creation, dissemination, copying, automated processing, and disposal of restricted MITRE information. Starting from the general idea that policy is a set of principles or plans that guide the actions taken by a person or group, we view policy in general as spanning requirements from high-level general guidance to detailed-level specific implementation directives. In the context of this task, the high-level guidance defines the general protection requirements for restricted MITRE information while, at the lowest level of detail, security implementation procedures provide the detailed implementation instructions that tell individuals what procedures to follow and how to properly use specific capabilities for automated processing.

In developing this policy we have used an approach of successive elaboration. The stages of elaboration are summarized in table 2. The proposed policy of this paper consists of the first two stages, encompassing general security requirements and their interpretation for the desktop processing environment.

The SPD task will address the third stage, the security paradigm, in a separate documentation product during fiscal year 1993. The security paradigm will identify security techniques and mechanisms that could support implementation of the proposed security policy. We call these techniques and mechanisms a security paradigm because they will provide a general example of how the proposed security policy might be implemented. The paradigm is not intended to be a set of requirements. Instead, it provides guidance in identifying products and procedures.

The final stage in the development of a complete policy will be to define a security implementation plan in terms of actual products and procedures that MITRE personnel should use. This final stage of policy specification will be done when the prototype capabilities are selected and installed in fiscal year 1994.

Thus, the first two stages in table 2 constitute the proposed policy of this paper, the third stage is a bridge between this policy and products, and the fourth stage defines the proper use of those products together with operating procedures.

Table 2. Stages of Elaboration in Development of Policy

Stage in Elaborating Security Requirements	Description
General Requirements	The general requirements specify employee responsibilities and general precepts for safeguarding restricted MITRE information.
Requirements for Desktop Processing	These requirements are interpretations of the general requirements for the automated desktop environment.
Security Paradigm	The security paradigm identifies techniques and mechanisms that could support implementation of the policy; the paradigm provides guidance for selecting products, it does not specify requirements.
Security Implementation Procedures	This stage specifies implementation in terms of actual products and procedures that MITRE personnel should use for automated processing of restricted MITRE information.

SPECIAL CONSIDERATIONS

In many of the requirements of the proposed security policy in the next section, reference is made to the MITRE Office of Good Practice (OGP). This term is being used in this paper as a generic designation for some MITRE organizational entity or combination of entities whose responsibilities will encompass those given in the proposed policy, such as evaluation of software, configuration control guidelines, audit, and evaluation of computing facilities to determine their suitability for processing restricted information.

PROPOSED SECURITY POLICY

GENERAL REQUIREMENTS

Employee Responsibilities

Employee 1 Any MITRE employee who intentionally intercepts wire or electronic communications without authorization, intentionally obtains access to information in networks or computers without authorization, or intentionally exceeds access permissions without authorization is in violation of the Electronic Communications Privacy Act of 1986 (US law) and is subject to criminal fines and penalties, civil damages, and corporate disciplinary action which may include termination of employment.

Employee 2 MITRE employees are responsible for safeguarding restricted MITRE information in accordance with MITRE policy[1]. Failure to do so is subject to corporate disciplinary action; intentional violation of the policy may also lead to termination of employment.

General Precepts for Safeguarding Restricted MITRE Information

Restricted MITRE information shall be created, used, and disposed of in accordance with the following safeguards.

Safeguard 1 — Creation Valid restricted MITRE information may be created when MITRE employees record facts, figures, ideas, plans, and so forth in the normal course of

[1] MITRE policy is currently defined in the MITRE Policy & Procedures, the MITRE Security Procedures handbook, the MITRE Personal Computer Policies and Procedures handbook, and various official memos that have appeared from time to time. When an official security policy for safeguarding restricted MITRE information, such as the one proposed in this document, is adopted by MITRE, it will become part of MITRE policy.

performing their jobs. Employees shall not create bogus restricted MITRE information in the guise of valid restricted MITRE information.

Safeguard 2 — Modification Restricted MITRE information may be modified by holders of such information who have a job-related need to process and update such information. Modification by others is not authorized: restricted MITRE information shall be protected from accidental modification, as well as rudimentary attempts at modification, by unauthorized individuals.

Safeguard 3 — Communication Restricted MITRE information may be disseminated by creators and holders of such information to MITRE employees who have a job-related need to know, use, hold, or process such information. Dissemination to others is not authorized: restricted MITRE information shall be protected from casual viewing as well as rudimentary attempts at viewing by unauthorized individuals.

Safeguard 4 — Transmission Restricted MITRE information may be transmitted by creators and holders of such information to MITRE employees who have a job-related need to know, use, hold, or process such information. Protection of the information against unauthorized disclosure and modification shall be appropriate to the medium used for transmission, as follows: US Postal Service and similar services are authorized for hard copy and diskettes; electronic transmission on the MITRE Corporate Network (MCN) (from sources within MITRE-controlled areas to destinations within MITRE-controlled areas) is authorized provided that adequate protection measures, as determined in approved interpretations of this policy, are employed. Electronic transmission of restricted MITRE information to destinations outside MITRE-controlled areas or on networks other than the MCN is not authorized.

Safeguard 5 — Removal From MITRE-Controlled Areas Removal of restricted MITRE information from MITRE-controlled areas is authorized for MITRE employees who otherwise have a need to use, hold, and process such information provided that they handle the information in accordance with MITRE policy.

Safeguard 6 — Storage Within MITRE-Controlled Areas Restricted MITRE information stored in MITRE-controlled areas shall be protected from casual viewing or modification, and from rudimentary attempts at unauthorized viewing or modification.

Safeguard 7 — Storage Outside MITRE-Controlled Areas Restricted MITRE information stored in nonMITRE-controlled areas shall be kept in a locked container and the length of time the information is stored in this manner shall be kept to the minimum consistent with legitimate performance of MITRE-related activities.

Safeguard 8 — Disposal Restricted MITRE information shall be disposed of in such a manner as to ensure that the information cannot easily be retrieved.

TECHNICAL REQUIREMENTS FOR DESKTOP PROCESSING

The policy for handling restricted-MITRE information in the desktop processing environment relies on several different kinds of technical capabilities for processing, storing, safeguarding, and transmitting information.

Suitability for Processing

Any personal workstation suitable for processing restricted MITRE information will satisfy the following requirements, as appropriate.

Personal Workstation 1 The computer shall provide its users the ability unambiguously to identify created objects (e.g., files, documents, spreadsheets, diskette contents) as containing or potentially containing restricted MITRE information.

Personal Workstation 2 The computer shall have a screensaver that is always enabled when the personal workstation is on. The screensaver shall satisfy the following requirements.

- The screen saver shall be configured to use a save-screen that completely hides the active information; the puzzle or flashlight type save-screens that move the active information around or move a small viewing area around the screen are not appropriate.

- The idle time before automatic activation of the screen saver shall be configured as one minute or less.

- The screen saver shall require a password to enable resumption of activity.

Personal Workstation 3 When restricted-MITRE information is deleted from the computer, tape, diskette, or similar media, the nonvolatile computer storage areas occupied by the deleted information, such as sectors and records on disks and tapes, shall be positively erased. If positive erasure of deleted areas used for deleted information is not done automatically by the computer, then the computer shall have suitable, approved utility software that can be invoked by the user to ensure positive erasure.

Suitability for Extended Storage

Suitability for storing restricted-MITRE information for extended periods requires, in addition to the above characteristics, the following provisions.

Personal Workstation 4 The computer must have one or more of the following capabilities: (a) a built-in lock that prevents use of the computer without the lock's key, (b) a login capability that requires, at minimum, a password for authentication of the user, or (c) the ability to convert all user-accessible restricted MITRE information to encrypted form via an encryption algorithm in the class of NIST's Data Encryption Standard (DES).

Suitability for Protection from Casual Observation or Modification

The following technical requirement makes suitable for restricted MITRE information a personal workstation that is used by unsupervised temporary users.

Personal Workstation 5 The computer must either have an access control capability that allows only predetermined, identified, and authenticated personnel to access designated objects or else must support the ability to maintain designated classes of objects in encrypted form (using DES or stronger encryption). We summarize this requirement by saying that the computer can protect objects from casual observation and modification.

Suitability for Network File Sharing

The capability for a user on one personal workstation to fetch documents from another personal workstation on the corporate network already exists in the MITRE environment. File sharing under System 7 for the Macintosh is typical of this capability.

File sharing is a combination of the desired functional capabilities for storing restricted information on personal workstations and sharing restricted information via the corporate network. Thus, most security aspects of file sharing are covered under the components of file sharing. However, file sharing involves the added element of access control, which is not dealt with under the storage and network transmission components of file sharing. It is addressed here.

Personal Workstation 6 Personal workstations providing file sharing capability shall have controls adequate to ensure that only designated individuals can access restricted MITRE information through the file sharing capability. Access control in this context shall provide control of confidentiality — only authorized individuals can view — and control of integrity — only authorized individuals can modify. Identification of the accessing entity shall be of an individual person, as opposed to identification of just the personal workstation being used to enable the file sharing. Most systems having user-level identification and authentication and file access controls in the form of access control lists or privilege bits provide adequate controls in this context. The file sharing capability provided with System 7.0.1 for the Macintosh, when used in a manner consistent with the policy in this document[2], provides adequate controls in this context.

[2] This means, for example, that the restricted information would have to be encrypted during transmission on the network.

Suitability for Network Transmission

Network 1 Personal workstations used to transmit restricted MITRE information on the MITRE Corporate Network shall have facilities for appropriately marking and encrypting such information, in that order. When there is a need to print such information and no networked printer is available that can properly decrypt the information, a dedicated printer may be used provided the user can satisfactorily verify that the printer is actually configured as a dedicated printer at the time of printing. Criteria for determining satisfactory verification will be provided for specific systems in the Security Implementation Procedures for this policy.

Network 2 Personal workstations used to transmit restricted MITRE information to a networked printer shall have the capability to ensure printout order of the transmitted information so that the user can be physically present at the time of printout to forestall inadvertent or intentional viewing of the information by unauthorized individuals.

USER RESPONSIBILITIES FOR DESKTOP PROCESSING

A **user** of a personal workstation is a MITRE employee who uses, maintains, or administers a personal workstation. Our policy distinguishes between **principal** users, who have a need to know restricted MITRE information, and **temporary users** such as secretarial personnel, administrators, PRISM personnel, Office of Good Practice (OGP) personnel, and other MITRE employees using the personal workstation to perform a service function on a limited time scale. Typically, a personal workstation has only one **principal** user who is often its principal maintainer as well. In the event that a home computer is used to process restricted MITRE information, the employee who lives in that home must own the computer, is both its **principal** user and its maintainer, and assumes all associated responsibilities.

In this context, a **maintainer** of a personal workstation is a MITRE employee who is responsible for the installation and maintenance of that computer. In some cases, maintainers may also be **administrators** who are responsible for allocation of computers, for ensuring that relevant technical requirements on computers and connecting networks are met, and for checking to be sure that they are used properly by their assigned users. Consequently, our user responsibilities for desktop processing are divided into three subcategories: responsibilities of principal users, responsibilities of maintainers, and responsibilities of administrators.

Responsibilities of Principal Users

Any principal user of a personal workstation is responsible for operating it in accordance with MITRE policy, as defined by the following user responsibilities.

Principal User 1 A user who creates an object containing restricted-MITRE information on a computer must do so in such a way as to unambiguously identify this fact.

Principal User 2 The user processing restricted-MITRE information shall physically arrange the personal workstation screen to inhibit casual viewing by passersby, workmen, or visitors.

Principal User 3 A user who writes restricted MITRE information to a diskette shall physically label the diskette with the marking "RESTRICTED-MITRE" and shall ensure that the volume label (name of the diskette stored on the diskette) includes the character string "RES-M". The user shall also ensure that the diskette is protected from casual, unauthorized viewing and from unauthorized modification until such time as the diskette is securely destroyed, manually conveyed to an appropriate recipient, or mailed to an appropriate recipient in a properly marked envelope.

Principal User 4 A user who prints restricted-MITRE information on a printer shall be physically present at the time of printing and shall ensure that the printed information is protected from casual, unauthorized viewing until such time as the printout is securely destroyed, conveyed to an appropriate recipient, or mailed to an appropriate recipient in a properly marked envelope.

Principal User 5 A user may electronically transmit restricted MITRE information but only on the trusted portion of the MITRE Corporate Network. The user shall ensure that the information is encrypted for transmission.

Principal User 6 A user who makes restricted-MITRE information available for retrieval over the MCN must ensure that the computer used is suitable for file sharing and must ensure that the file sharing access controls provided by the computer are properly employed.

Principal User 7 If a user leaves restricted-MITRE information stored on a personal workstation in a MITRE-controlled area for extended periods (e.g., overnight, during weekend idle times), then the computer must be suitable for storing restricted-MITRE information and the user must do one (or more) of the following: (a) lock the computer using a physical key; (b) enable its approved login capability or (c) store all user-accessible restricted-MITRE information using its approved encryption mechanism and keys that are not available to unauthorized personnel.

Principal User 8 Restricted-MITRE information on a personal workstation shall be protected from casual viewing and modification by temporary users in one of the following ways:

- A principal user of the computer shall be present whenever a temporary user is working at the computer,.shall instruct the temporary user to avoid restricted-

MITRE information objects, and shall verify by observation that the objects are not viewed.

- A computer suitable for protecting information from casual observation and modification shall be used. Each principal user of the computer shall protect restricted-MITRE information stored on the computer from casual observation by temporary users through the use of available access controls and/or encryption techniques. If encryption techniques are used, the principal user shall use encryption keys that are not known to, or available for use by, temporary users.

Principal User 9 No user shall store restricted-MITRE information on a personal workstation for extended periods except in a MITRE-controlled area or in a home computer for which the employee is the principal user, maintainer, and administrator and only if the employee has explicitly agreed to ensure that all the duties and responsibilities of those roles are properly executed. However, diskettes and portable personal workstations containing restricted-MITRE information can be left unattended in nonMITRE areas for short periods of time, not to exceed twenty-four hours, if they are physically stored in a lockbox, such as an airport lockbox.

Principal User 10 A MITRE employee having a legitimate need to use restricted-MITRE information is authorized to move such information between a MITRE-controlled area and another area, and to process it in the other area, provided:

- The other area is either a MITRE work place, even though the physical area may not be under MITRE control, or an area under the employee's control, such as the employee's home.

- The computer used for processing meets the suitability requirements for processing and, if relevant, storing restricted-MITRE information.

- Storage media used to transfer information (e.g., diskettes) are physically protected by the employee.

Principal User 11 When a MITRE employee discards diskettes or other permanent storage media, the employee shall ensure that all restricted MITRE information has first been positively erased from the media before disposal.

Responsibilities of Maintainers

The maintainers of a personal workstation are responsible for configuring and operating that computer in accordance with MITRE policy, as defined by the following maintainer responsibilities. Principal users are generally authorized to install software, perform maintenance functions, and assume the additional responsibilities assigned to maintainers.

Maintainer 1 Maintainers shall include Office of Good Practice (OGP)-approved anti-virus software with any new personal workstation installation that is to be used to process or store restricted-MITRE information and shall ensure that this software is maintained in accordance with OGP standards.

Maintainer 2 Maintainers shall install only OGP-approved software in personal workstations that process or store restricted-MITRE information. Software purchased or otherwise legitimately obtained by an employee may be installed and used only on approval of OGP. Software created and controlled by a principal user of a personal workstation is authorized for that computer provided it is appropriately registered for purposes of configuration control. Freeware and shareware software are not authorized in this context unless supplied by OGP.

Maintainer 3 Maintainers shall follow OGP-established configuration control guidelines for personal workstations processing restricted-MITRE information.

Responsibilities of Administrators

As outlined below, administrators of personal workstations have responsibilities for ensuring that they are operated in accordance with MITRE policy.

Administrator 1 The administrator of a personal workstation shall ensure that its assigned users have a legitimate need to use the personal workstation and the information resources which it makes available to them. The administrators shall be able to advise the computer's principal users as to whether the computer and any connected networks are deemed, by OGP, to be suitable for processing and transmitting restricted-MITRE information.

Administrator 2 Administrators shall assign computers for the purpose of storing restricted-MITRE information for extended periods of time only when such computers reside in MITRE-controlled areas and are deemed by OGP to be suitable for the storage of this information.

Administrator 3 If administrators grant passwords to temporary users of a computer used to process restricted-MITRE information, they shall ensure that the computer has the capability to protect information from casual observation as described elsewhere in this policy.

CORPORATE RESPONSIBILITIES FOR DESKTOP PROCESSING

Corporate 1 The MITRE Office of Good Practice (OGP) shall establish configuration control guidelines for personal workstations processing restricted-MITRE information. These guidelines shall ensure that maintainers and administrators are adequately informed of technical capabilities of approved hardware and software. They shall ensure that approved software usage does not involve unexpected side effects that could cause inadvertent loss of security markings or transmission of restricted-MITRE information.[3]

Corporate 2 The MITRE Corporation shall conduct periodic audits of all employees' personal workstations to verify that they are properly configured for the kind of information they are authorized to process and that they are being used in accordance with MITRE policy. The administrator who audits the use of a given computer shall in no case be a principal user of that computer.

Corporate 3 This security policy shall be publicly available and shall periodically be reviewed by security experts both within MITRE and within the larger security community. These reviews shall provide a basis for periodic policy updates.

THREAT ANALYSIS

Threats of primary concern include accidental actions resulting from improper configurations, unmarked information containers, casual viewing, and laxity in maintaining proper configurations. These threats must be considered both within MITRE-controlled areas and in other areas where restricted-MITRE information might be stored or processed. Outside MITRE-controlled areas, premeditated attacks must also be considered.

Premeditated attacks by ill-motivated MITRE employees, such as systematic exploitation of product vulnerabilities or traffic analysis on networks, are certainly within the realm of possibility but no technical countermeasures are considered on the grounds of severe imbalance between cost and benefit. Also, such attacks are considered to be only remotely possible and other, more direct measures seem more likely to be used by an ill-motivated employee. Likewise, exotic attacks by outsiders, such as analysis of electromagnetic emanations, are discounted.

Thus, we consider threats to confidentiality of the restricted MITRE information and threats to the integrity of both the information and the personal workstations involved in processing it.

[3] The security properties of approved software should be self-evident to the user. It is important that security not depend too much on whether ordinary users are paying attention to security bulletins from PRISM. Thus, there is no user responsibility that mentions PRISM.

THREATS TO CONFIDENTIALITY

Passive Observation

Threat Personal workstations' screens may be visible to passersby, workmen, and visitors who do not have a need to know restricted-MITRE information.

Countermeasures Physical placement during actual use inhibits this, by responsibility **Principal User 1**. Use of an effective screensaver inhibits this at other times, by requirement **Personal Workstation 2**.

Threat Information transmitted on the MITRE Corporate Network (MCN) may be captured and viewed by MITRE employees engaged in legitimate monitoring of the MCN.

Countermeasures This is inhibited by use of encryption techniques, as specified in network processing requirement **Network 1**.

Threat Casual viewing by an unauthorized person of restricted-MITRE information in a printout on a networked printer can easily occur. This is especially true when a document is printed on a networked printer using Print Monitor under the Macintosh System 7 operating system because the user cannot predict when the document will appear in the output hopper. In any case, the document, especially if it consists of a small number of pages, can easily be taken inadvertently by another user whose printouts sandwich the document in question.

Countermeasures The use of networked printers is explicitly ruled out by processing requirement **Network 2**. Dedicated printed printers must be physically guarded during printing, by responsibility **Principal User 4**.

Threat Temporary users may, in the absence of protection measures, inadvertently view restricted information they should not have access to.

Countermeasures Responsibility **Principal User 8** directly addresses this threat by requiring either direct supervision of temporary users or the effective use of controls on computers that are suitable for protecting information from casual observation.

Threat Permanent storage media, such as hard disks and diskettes, containing restricted-MITRE information may be discarded and thereby become available to unauthorized recipients.

Countermeasures This possibility is explicitly ruled out by responsibility **Principal User 10**; the technical ability to purge unwanted information is, itself, made possible by requirement **Personal Workstation 3**.

Coincidental Actions

Threat Personal workstation users, maintainers, or administrators may make mistakes or become lax in maintaining and operating their personal workstations. Also, they may fail to notice that changes in security implementation requirements have occurred. Laxity and inattention increase the risk that inappropriate communication or dissemination of restricted MITRE information may occur through procedural or software actions.

Countermeasures Mistakes are inhibited when maintainers follow (responsibility **Maintainer 3**) management guidelines established by OGP (responsibility **Corporate 1**). Errors in following these guidelines are corrected in the course of corporate auditing (responsibility **Corporate 2**). Laxity is countered by public dissemination and review of policy (responsibility **Corporate 3**).

Threat Restricted-MITRE information that is not adequately marked as being restricted-MITRE information might accidentally be disclosed. For example, a diskette might accidentally be disclosed if the diskette is not clearly marked as containing restricted-MITRE information.

Countermeasures Marking of computer-resident and diskette-resident information is covered by requirement **Personal Workstation 1** and responsibility **Principal User 3**. Marking of information transmitted over networks is covered by network processing requirement **Network 1**. The need to directly mark printed hard copy is avoided through the somewhat stringent user responsibility **Principal User 4**. The user responsibilities in this area are supported by requirement **Administrator 1**.

Threat In a computer that supports file sharing, the wrong person might get restricted information through a network fetch. This is a potential concern even in MITRE-controlled areas.

Countermeasures Such a com;uter must be suitable for file sharing by requirements **Personal Workstation 6**, **Administrator 1**, and **Principal User 6**.

Threat Improper configurations of hardware and software, unreliable software, software of unknown origin, and improper operation can contribute to or directly cause inappropriate dissemination of restricted-MITRE information.

Countermeasures Improper configuration and unsuitability of software is addressed through OGP configuration-management guidelines (responsibility **Corporate 1**) and maintenance responsibilities **Maintainer 1** through **3**.

Exploitation of Product Vulnerabilities

Threat In MITRE-controlled areas there is the small chance that employees or other personnel on MITRE premises during off-hours might be tempted to obtain information from an unattended personal workstation or might accidentally view restricted MITRE information while using the personal workstation for their own purposes. A sophisticated user might even go so far as to examine "deleted" information that has not yet been erased using a disk-recovery utility; some operating environments, such as MS-DOS 6.0, even have built-in undelete capabilities usable by anyone.

Countermeasures This threat of rudimentary snooping is countered by requirement **Personal Workstation 4** and user responsibility **Principal User 7**.

Attacks by Outsiders

Threat In public places there is the chance that an unattended personal workstation might be stolen and subjected to professional attempts at viewing restricted-MITRE information, including apparently "deleted" information.

Countermeasures This threat is countered by prohibiting storage of restricted-MITRE information outside of MITRE-controlled areas without adequate physical or access control safeguards (suitability requirement **Personal Workstation 4** and responsibilities **Principal User 9** and **10**).

Threat In public places there is the chance that an unattended personal workstation might be altered and thereby subjected to later, professional attempts at viewing restricted-MITRE information.

Countermeasures This threat is countered by the prohibition against leaving the personal workstation unattended unless kept in a lockbox (**Principal User 9**). In addition, corporate auditing responsibility could be strengthened to cover detection of tampering, such as software or hardware implants.

THREATS TO INTEGRITY

Passive Modification

Threat Temporary users may, in the absence of protection measures, inadvertently modify restricted information they should not have access to.

Countermeasures Responsibility **Principal User 8** directly addresses this threat by requiring either direct supervision of temporary users or the effective use of controls on computers that are suitable for protecting information from casual modification.

Coincidental Actions

Threat Personal workstation users, maintainers, or administrators may make mistakes or become lax in maintaining and operating their personal workstations. Also, they may fail to notice that changes in security implementation requirements have occurred. Laxity and inattention increase the risk that inappropriate modification of restricted MITRE information may occur through procedural or software actions.

Countermeasures Mistakes are inhibited when maintainers follow (responsibility **Maintainer 3**) management guidelines established by OGP (responsibility **Corporate 1**). Errors in following these guidelines are corrected in the course of corporate auditing (responsibility **Corporate 2**). Laxity is countered by public dissemination and review of policy (responsibility **Corporate 3**).

Threat Restricted-MITRE information that is not adequately marked as being restricted-MITRE information might accidentally be modified. For example, a diskette might accidentally be modified if the diskette is not clearly marked as containing restricted-MITRE information.

Countermeasures Marking of computer-resident and diskette-resident information is covered by requirement **Personal Workstation 1** and responsibility **Principal User 3**. Marking of information transmitted over networks is covered by network processing requirement **Network 1**. The need to directly mark printed hard copy is avoided through the somewhat stringent user responsibility **Principal User 4**. The user responsibilities in this area are supported by requirement **Administrator 1**.

Threat In a computer that supports file sharing, the wrong person might modify restricted information through the file sharing capability. This is a potential concern even in MITRE-controlled areas.

Countermeasures Such a computer must be suitable for file sharing by requirements **Personal Workstation 6, Administrator 1**, and **Principal User 6**.

Threat Improper configurations of hardware and software, unreliable software, software of unknown origin, and improper operation can contribute to or directly cause inappropriate modification of restricted-MITRE information.

Countermeasures Improper configuration and unsuitability of software is addressed through OGP configuration-management guidelines (responsibility **Corporate 1**) and maintenance responsibilities **Maintainer 1** through **3**.

Exploitation of Product Vulnerabilities

Threat In MITRE-controlled areas there is the small chance that employees or other personnel on MITRE premises during off-hours might be tempted to modify information on an unattended personal workstation or might accidentally modify restricted MITRE information or otherwise corrupt the integrity of the computer system while using the personal workstation for their own purposes. A sophisticated user might even go so far as to implant a Trojan horse.

Countermeasures This threat of rudimentary attack on the integrity of information or software is countered by requirement **Personal Workstation 4** and user responsibility **Principal User 7**.

Attacks by Outsiders

Threat In public places there is the chance that an unattended personal workstation might be stolen and subjected to professional attempts at modifying restricted-MITRE information or the software of the personal workstation.

Countermeasures This threat is countered by prohibiting storage of restricted-MITRE information outside of MITRE-controlled areas without adequate physical or access control safeguards (suitability requirement **Personal Workstation 4** and responsibilities **Principal User 9** and **10**).

Threat In public places there is the chance that an unattended personal workstation might be altered and thereby subjected to later, professional attempts at modifying restricted-MITRE information or otherwise corrupting the configuration or operation of the personal workstation.

Countermeasures This threat is countered by the prohibition against leaving the personal workstation unattended unless kept in a lockbox (**Principal User 9**). In addition, corporate auditing responsibility could be strengthened to cover detection of tampering, such as software or hardware implants.

Threat Access to MITRE-owned computers by outsiders, even in the absence of any actual disclosure or modification of information or damage to software, could be used by the press or others as a vehicle to embarrass the MITRE Corporation for lack of prudent security management.

Countermeasures The MITRE Corporation clearly cannot prevent people from maligning it. However, the Corporation can be prepared to suppress erroneous information with factual counterclaims. This is the primary motivation for responsibility **Corporate 3**.

LIST OF REFERENCES

1. PRISM, May 1993, *Personal Computer Policies and Procedures*, The MITRE Corporation, Bedford, Massachusetts.

2. *MITRE Policies and Procedures*, The MITRE Corporation, Bedford, Massachusetts: Section B.2.a — Handling of Sensitive/Regulatory and Proprietary Information 30 September 1988; Section B.2.e — Protection of Unclassified Computers and Data Communications Systems, 17 July 1991; Section F.1.c — Identification of Privileged Correspondence or Communications, 30 September 1988.

3. *MITRE Security Procedures*, 1988, M88-25, The MITRE Corporation, Bedford, Massachusetts: Section 23 — Unclassified Computers and Data Communications Systems; Section 24 — Automated Information Systems.

GLOSSARY

Anti-Virus Software: Software that detects and/or neutralizes computer viruses.

Automated Information System: An assembly of computer hardware, software, and firmware configured to automate the functions of calculating, computing, sequencing, storing, retrieving, displaying, communicating, or otherwise manipulating data, information, and text material.

Availability: The idea that information or automated processing capabilities are where a user needs them, when the user needs them, and in the form needed by the user.

Classified Information: Official information, including foreign classified information, that has been designated as requiring protection in the interest of national security.

Confidentiality: The idea of holding sensitive information in confidence, limited to an appropriate set of individuals or organizations.

For Official Use Only (FOUO): A government marking that indicates information is not approved for public release.

Integrity:

of Data — (1) The property that data meet some predefined expectation of quality.

(2) The state that exists when the quality of stored information is protected from contamination or degradation by information of lower quality.

of a System or Process — The quality that a system or process has when it performs its intended function in an unimpaired manner, free from deliberate or inadvertent, unauthorized manipulation.

MITRE Policy on Safeguarding Restricted MITRE Information: MITRE policy is currently defined in the MITRE Policy & Procedures, the MITRE Security Procedures handbook, the MITRE Personal Computer Policies and Procedures handbook, and various official memos that have appeared from time to time. When an official security policy for safeguarding restricted MITRE information, such as the one proposed in this document, is adopted by MITRE, it will become part of MITRE policy.

Need-to-Know (for unclassified information): A determination made by the owner or holder of protected information that a prospective recipient has a legitimate need to access the protected information.

Personal: For use on official correspondence contained in envelopes marked TO BE OPENED BY ADDRESSEE ONLY. This particular designation may be used by any department, but is most frequently used by Corporate Officers, Directors, the Office of Human Resources, or the Finance and Accounting Department, when a high degree of privacy is required.

Personal Computer: Any computer system that runs a DOS-based, Windows-based, or Macintosh operating system and has an IBM PC-compatible or Apple processor. (This definition is intended to exclude a system such as a SUN workstation emulating a Macintosh computer.)

Personal Workstation: Any personal computer (as defined in this glossary) as well as UNIX-based desktop computers such as SUN workstations.

Privileged: Used for official correspondence and mail covers when a degree of privacy is required. This type of marking must be controlled by an attached distribution list, and the document must be locked up when not in use. Material in this category should be disposed of in a classified waste receptacle. Correspondence with this designation may be opened by secretarial or clerical personnel when in line with their assigned responsibilities.

Proprietary Information: Information which, in the judgment of the owner, could jeopardize the owner's competitive position if released to others, particularly to competitors. Proprietary documents should be identified as such by the owner. This is usually done by marking "PROPRIETARY" on the cover or title page.

Restricted MITRE Information: Information about MITRE, including its plans, its finances, and its personnel, which for reasons of ordinary prudence, inherited responsibility, or privacy of the corporation or individuals should be restricted to viewing and handling by authorized individuals only. Restricted MITRE information includes executive, financial, and personnel information. General identification of authorized individuals and appropriate controls is given in MITRE policy covering this category of information.

Sensitive Information: Information that sources require to be closely held, whether for competitive, policy, governmental, or other lawful reasons. Example of markings that may appear on sensitive information include PRIVILEGED, COMPANY PRIVATE, FOR OFFICIAL USE ONLY (FOUO), or their equivalents expressed in a foreign language. In some instances, sensitive information may not be clearly marked, or may be unmarked and its sensitivity conveyed contractually or verbally. Examples include financial reports, cost data, corporate plans, new design concepts, bids, proposals, and contracts. In any event, such information must be handled as *Sensitive* information. In the context of this paper, a piece of information is sensitive if its mishandling is a material threat to MITRE or its employees or customers.

Trojan Horse: A computer program with an apparently or actually useful function that contains additional, hidden functions that surreptitiously exploit the legitimate authorizations or privileges of the invoking process resulting in loss of confidentiality, integrity, or availability.

To Be Opened by Addressee Only: Used for mail covers only and not on official correspondence or contents. This particular designation may be used by any department, but is most frequently used by Corporate Officers, Directors, the Office of Human Resources, or the Finance and Accounting Departments. This protective designation is intended to restrict the handling of the contents to the named addressee only and may not be opened by secretarial or clerical personnel.

Virus: A self-propagating Trojan horse, normally composed of a mission component, a trigger component, and a self-propagating component.

Workstation: Generally used to indicate any desktop-type computer system including, for example, personal computers (as defined in this glossary) as well as UNIX-based desktop computers, SUN workstations, and a variety of special-purpose or very high performance desktop systems.